COMMENTS

This Amendment is submitted in response to a June 23, 2010 non-final Office Action. The present Amendment amends **Claims 12 and 22-24**. **Claims 1-3, 5-9, 11-14, 16, and 22-24** are currently pending.

In this Amendment, Applicants have amended **Claims 12 and 22-24**. Applicants are not conceding that the subject matter encompassed by the claims prior to this Amendment is unpatentable over the art cited by the Examiner. Applicants respectfully reserve the right to pursue claims in one or more continuing applications, including claims capturing the subject matter encompassed by Claims 1-3, 5-9, 11-14, 16, and 22-24 prior to this Amendment and additional claims.

Rejections Under 35 U.S.C. § 101

In paragraph 4 of the present Office Action, **Claims 12-14 and 16** are rejected for potentially claiming non-statutory transitory signals. The present amendment adopts the Examiner-suggested language of "non-transitory computer storage medium." Thus, Applicants respectfully request that these rejections be withdrawn.

Rejection Under 35 U.S.C. § 112

In paragraph 23 of the present Office Action, **Claim 23** is rejected for lack of antecedent basis for the term "the DHCP server." Claim 23 had a typographical error, in which it depended on **Claim 1**, instead of **Claim 22**, which provides the proper antecedent basis. The present amendment addresses this issue, and thus Applicants respectfully request that this rejection be withdrawn.

Rejections Under 35 U.S.C. § 103

In Paragraph 8 of the present Office Action, **Claims 1-5, 7-9, 11-14, 16, and 22-24** are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Hanson, et al.* (U.S. Patent Application Publication No. 2003/0120811 – "*Hanson*") in view of *Doherty, et al.* (U.S. Patent Application Publication No. 2003/0018763 – "*Doherty*"). In paragraph 9 of the present Office Action, **Claim 6** is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Hanson* and *Doherty*, and further in view of *Giglio, et al.* (U.S. Patent Application No. 2004/0039821 – "*Giglio*"). In paragraph 10 of the present Office Action, **Claim 24** is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Hanson* and *Doherty*, and further in view of *Khaki, et al.* (U.S. Patent No. 6,067,569 – "*Khaki*"). Applicants respectfully traverse these rejections.

Hanson teaches that a client computer can receive an IP address from a DHCP server. (See cited paragraphs [0286] – [0288].)

Doherty teaches that the DHCP and bootstrap protocol permit a client computer to automatically contact a server. This server can then send a boot program to the client. (See cited paragraph [0006] of *Doherty*).

Giglio teaches that a network administrator can oversee the operations of devices on a network. (See cited paragraph [0007] of *Giglio*.)

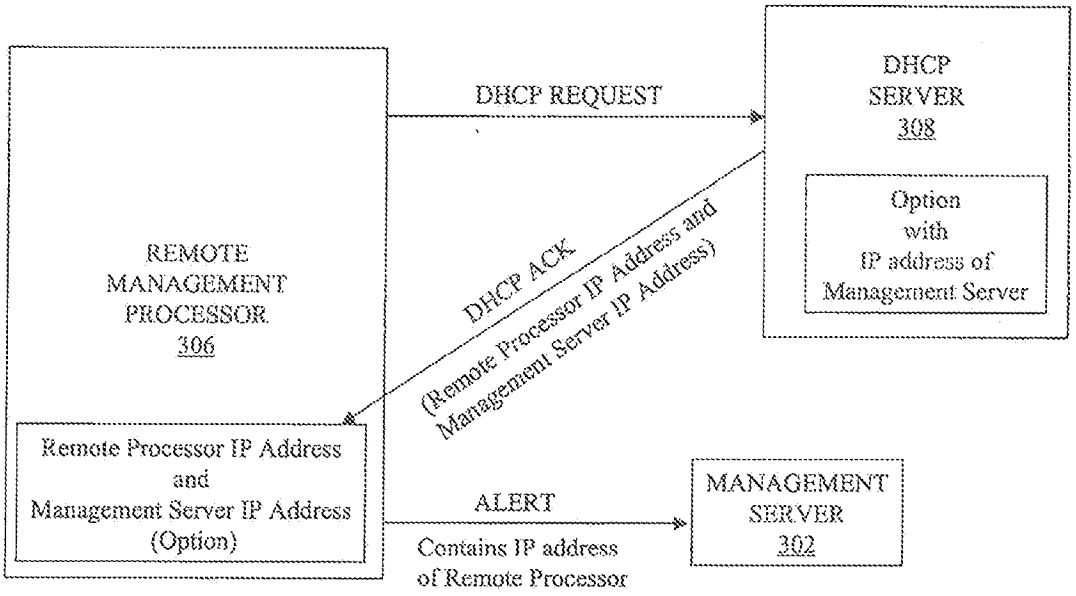
Khaki teaches that a network card (NIC) can communicate without using the operating system of the CPU in the computer to which it is attached. (See cited col. 2, line 59 to col. 3, line 8 and Claim 24 of *Khaki*.)

With reference to exemplary **Claim 1**, a combination of the cited art does not teach or suggest:

"in response to the detecting of the Option data, automatically sending the alert packet to the destination address" (of the management server) "by the at least one remote management processor, such that the alert packet includes the received requested IP address of the at least one

remote management processor," as supported in the present specification on page 6, lines 14-18, and in FIG. 3 of the present specification.

Consider now FIG. 3 of the present application:



When remote management processor 306 (i.e., a client of a DHCP server) requests an IP address from DHCP server 308, the DHCP server 308 sends a packet to the remote management processor 306. This packet contains not only the newly-assigned IP address for remote management processor 306, but it also includes Option data. This Option data includes the address of management server 302. By extracting the address of management server 302 from the Option data, remote management processor 306 can send management server 302 an alert, letting management server 302 know that remote management processor 306 has received its requested IP address from DHCP server 308. (See page 6, lines 1-18 of the present specification.)

A combination of the cited art does not teach or suggest the feature of a client (i.e., the remote management processor 306) sending an IP address of a remote management processor to

a management server, as presently claimed. The final Office Action cites paragraphs [0287] – [0288] of *Hanson* as teaching this feature. This cited passages states:

> [0286] It is common to use a Dynamic Host Configuration Protocol (DHCP) to automatically configure network devices that are newly activated on such a subnet. For example, a DHCP server on the sub-net typically provides its clients with (among other things) a valid network address to "lease". DHCP clients may not have permanently assigned, "hard coded" network addresses. Instead, at boot time, the DHCP client requests a network address from the DHCP server. The DHCP server has a pool of network addresses that are available for assignment. When a DHCP client requests a network address, the DHCP server assigns, or leases, an available address from that pool to the client. The assigned network address is then "owned" by the client for a specified period ("lease duration"). When the lease expires, the network address is returned to the pool and becomes available for reassignment to another client. In addition to automatically assigning network addresses, DHCP also provides netmasks and other configuration information to clients running DHCP client software. More information concerning the standard DHCP protocol can be found in RFC2131.
>
> [0287] Thus, when a Mobile End System 104 using DHCP roams from one subnet to another, it will appear with a new network address. In accordance with the present invention, Mobile End Systems 104 and Mobility Management Server 102 take advantage of the automatic configuration functionality of DHCP, and coordinate together to ensure that the Mobility Management Server recognizes the Mobile End System's "new" network address and associates it with the previously-established connection the Mobility Management Server is proxying on its behalf.

As highlighted, the cited passage states that a Mobility Management Server 102 can recognize the new network address of a client (Mobile End System 104). "How" the Mobility Management Server 102 actually obtains that new network address of the client (or even knows that such an address has been assigned) is taught in paragraph [0289], which states:

> [0289] The present invention provides DHCP listeners to monitor the DHCP broadcast messages and thereby ascertain whether a particular Mobile End System 104 has roamed from one subnet to another and is being offered the ability to acquire a new network address by DHCP.

As further clarified in paragraph [0300] of *Hanson*, information about the new IP addresses is "continually updated based on DHCP broadcast traffic appearing on network 108."

That is, the Mobility Management Server 102 "listens" for data traffic from the DHCP server, which broadcasts new IP addresses onto the network. If the Mobility Management Server 102 recognizes one of the IP addresses as being sent to a client that it supervises, then it makes a note as such. Thus, in *Hanson* the client's new IP address is sent from the DHCP server to the Mobility Management Server, NOT from the client (i.e., the presently claimed remote management processor) to the Mobility Management Server (i.e., the presently claimed management server 302). Thus, the feature of sending the alert packet to the destination address ("IP address of the management server") by the at least one remote management processor, such that the alert packet comprises the received requested IP address of the at least one remote management processor is not taught or suggested. Note that the distinction is not trivial, since the presently claimed invention allows the client (i.e., remote management processor) to control what information its management server receives.

In the present Office Action, the Examiner cites a single line from *Hanson* in paragraph [0287] as teaching/suggesting that the client tells the management server what the client's new IP address is. This line states that the "Mobile End Systems 104" (i.e., a client) "and the Mobility Management Server 102" (i.e., a management server) "coordinate together to ensure that the Mobility Management Server recognizes the Mobile End System's "new" network address and associates it with the previously-established connection the Mobility Manager Server is proxying on its behalf." However, there is no teaching or suggestion that coordinate together means that the client (Mobile End Systems 104) sends its new IP address to the management server (Mobility Management Server 102). Rather, the Mobility Management Server 102 obtains the client's IP address from the broadcast of IP addresses from the DHCP server (as described in paragraph [0308] of *Hanson*):

> [0308] In the preferred embodiment, all Mobile End Systems 104 transmit the same Client Identifier and Hardware Address in DHCP Discover requests. This allows the listener data structures and associated processes to distinguish Mobile End System-originated Discover requests from Discover requests initiated by other network devices. Likewise, the DHCP server will broadcast its response, so any Mobile End System 104 and/or the Mobility Management Server 102 will be able to pick up the DHCP server Offer response to any other Mobile End System. Since multiple DHCP servers can respond to a single DHCP Discover message,

the listener data structures shown in FIG. 16 store each server response in a separate data block, tied to the main handle via linked list. (Emphasis added.)

Thus, Applicants respectfully requests that the rejection of **Claims 1-3, 5-9, 11-14, 16, and 23** be withdrawn, and that **Claims 1-3, 5-9, 11-14, 16, and 23** be allowed to issue.

With respect to **Claim 22**, a combination of the cited art does not teach or suggest "the DHCP server transmitting a requested client IP address, a shelf life of the requested client IP address, and a management server address to the client, wherein the management server address is an IP address of a management server that monitors operations of the client, and wherein the management server address enables the client to transmit the requested client IP address and the shelf life of the requested client IP address to the management server," as supported in the present specification on page 6, lines 10-18.

More specifically, a combination of the cited art does not teach or suggest the DHCP server transmitting a management server IP address to the client, where the management server monitors operations of the client. As described above, *Hanson* (e.g., in paragraph [0286]) teaches a system in which a DHCP server sends a client IP address to that client. There is no teaching or suggestion of the DHCP server sending a management server IP address to the client that is being monitored by that management server, and wherein the management server address enables the client to transmit the requested client IP address and the shelf life of the requested client IP address to the management server.

With respect to **Claim 24**, a combination of the cited art does not teach or suggest "wherein the alert packet is transmitted from said at least one remote processor without said at least one remote processor loading an operating system," as supported in the original specification in paragraph [0020]. The present Office Action cites col. 2, line 59 to col., 3, line 8, and Claim 24 of *Khaki* for teaching this feature. The cited passages state:

In accordance with a first aspect of the present invention, a method of fast-forwarding a network packet is performed in a general-purpose computer system. "Fast-forwarding" refers to the network card performing the routing rather than a

main central processing unit performing the routing. The computer system has a main central processing unit and a network card for interfacing the computer system with multiple networks. The network packet is received in the network card and is destined to a selected one of the networks. The received network packet is analyzed by the network card to determine whether the network packet should be fast-forwarded to its destination network by the network card or alternatively, routed by the main central processing unit. When it is determined that a network packet should be fast-forwarded to the destination network by the network card, it is fast-forwarded without intervention of the main central processing unit. (Emphasis added.)

24. The method of claim 22, further comprising maintaining a fast-forwarding cache by the network driver for use when analyzing, the fastforward cache having routing information which is accessed to determine which network packets are to be transmitted by the network card without intervention from the operating system.

Thus, the cited passages state that a network card can function without using the CPU of the computer (and that CPU's O/S) to which the network card is attached. There is no teaching or suggest of the processor ("at least one remote processor") transmitting a packet without having loaded an O/S ("without said at least one remote processor loading an operating system").

CONCLUSION

As the cited prior art does not teach or suggest all of the limitations of the pending claims, Applicants now respectfully request a Notice of Allowance for all pending claims.

If the Examiner believes that an additional telephone call would be useful in promoting the pending claims to allowance, a call to the undersigned at 512.306.0796 would be greatly appreciated.

No additional extension of time, beyond that requested above, for this response is believed to be necessary. However, in the event any additional extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application to **IBM CORPORATION DEPOSIT ACCOUNT No. 50-0563**.

Respectfully submitted,

James E. Boice
Registration No. 44,545
LAW OFFICE OF JIM BOICE
3839 Bee Cave Road
Suite 201
Austin, Texas 78746
512.306.0796
ATTORNEY FOR APPLICANT(S)